REMARKS

The foregoing amendments are responsive to the August 23, 2005 Office Action. Applicant respectfully request reconsideration of the present application in view of the foregoing amendments and the following remarks.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Amendments to the Specification

A new substitute specification is provided herewith. Although a first substitute specification was provided by the Applicant in a previous amendment, the first substitute specification still contained numerous grammatical informalities. The present substitute specification does not add any new matter. Rather the present substitute specification fixes the numerous grammatical informalities in the previous specifications, including the specific informalities identified by the Examiner in the Final Office Action.

Response to Objection of Claims 13-17

The Examiner objected Claims 13-17 due to various informalities. Claims 13-16, 18-25 and 27-28 have been amended to correct a number of grammatical informalities and to further clarify the claimed invention.

Regarding Named Inventor on the Japanese Priority Applications

Enclosed please find certified copies of the Japanese priority applications JP 2000-299305 and 2001-161754. The Examiner questioned why the name shown on the Japanese Priority applications spelled differently than the name on the present U.S. Application.

Applicant is the named inventor on the Japanese priority applications. Applicant's Chinese name is 高振宇, which translates in English to Zhenyu Gao. However, in translation from Japanese kanji to English, the spelling of Applicant's name became Ko Shinu. Thus, the English version of the Japanese priority documents show Applicant's name as translated from Chinese to Japanese to English. Applicant is the inventor of the Japanese priority applications and has declared such on the Inventors Declaration filed in this application.

Response to Rejection of Claims 13-15 Under 35 U.S.C. 103(a)

The Examiner rejected Claims 13-15 under 35 U.S.C. 103(a) as being unpatentable over Scott (U.S. Publication No. 20010044820), further in view of Groshon et al. (U.S. Patent No. 6,351,811), further in view of Bianco (European Patent No. 467,239) and further in view of Blickenstaff et al. (U.S. Patent No. 5,537,585).

Scott teaches a file scanning type of system wherein files are scanned at a scanning frequency. In the system of Scott, there is a window of opportunity for transmission of improperly modified data. This window of opportunity opens when the file is improperly modified and does not close until the file scan checks the modified file. During this window of opportunity, data from an improperly modified file will be sent to a requestor.

Groshon teaches a system wherein a digital signature associated with requested data is compared to a control signature. However, in Groshon the web page data is not protected by being encrypted. Further, in Groshon the backup web page storage is not protected from an attacker. In Groshon, the backup web page storage is directly available to the web server and, thus, available to be modified by an attacker.

By contrast, in Applicant's system the web content stored on the public server is protected by being encrypted. The backup web content is protected from attack because it is not directly accessible from the public server and, thus, not accessible by an attacker. The backup web content is provided to a private server which is separated from the public server by a firewall. When unauthorized modification of the encrypted content on the public web server is detected, the encrypted copy can be restored by sending a request to the protected private server. No combination of Scott and Gerson with the other references teaches such a system wherein the public content is protected by encryption and the private content is protected behind a firewall.

Regarding Claim 13, the cited prior art does not teach or suggest an anti-alteration system for web-content having a public-web-server configured to create safe-web-files encrypted from original web-contents including one or more types of static files and one or more types of dynamic file, and configured to provide HTTP web server functions, a private-web-server configured to provide the original web-content the public-web-server provided to the private-web-server through a firewall, wherein when a web visitor's request is received, the public-web-server is configured to verity that the safe-web-file has not been improperly altered, deleted or replaced, the public-web-server further configured to decrypt one or more of the safe-web-files and respond to the visitor, and the public-

web-server further configured to automatically send a recovery request to the private-web-server when the public-web-server detects an unauthorized alteration of the safe-web-files, the private-web-server, in response to the recovery request, configured to send the safe-web-files to the public server.

Regarding Claim 14, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 13, wherein the encryption comprises chaos encryption technology to do encryption and decryption of the web-content for increasing the web server response speed and increasing security strong of whole system.

Regarding Claim 15, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 13, further comprising a real-time-check module used on the public-web-server computer for linking to a decryption module, wherein the decryption module is configured to decrypt one or more of the safe-web-files in response to an HTTP request received from the web visitor.

Accordingly, Applicant asserts that Claims 13-15 are allowable over the prior art, and Applicant requests allowance of Claim 13-15.

Response to Rejection of Claims 16-28 Under 35 U.S.C. 103(a)

The Examiner rejected Claim 16-28 under 35 U.S.C. 103(a) as being unpatentable over the modified Scott, Groshon et al., Bianco, and Blickenstaff et al. system as applied to Claim 1 above, further in view of Menezes et al. (Handbook of Applied Cryptography) and further in view of Thomson (U.S. Patent No. 5,276,874).

As described above, Groshon teaches a system wherein a digital signature associated with requested data is compared to a control signature. However, in Groshon the web page data is not protected by being encrypted. Further, in Groshon the backup web page storage is not protected from an attacker. In Groshon, the backup web page storage is directly available to the web server and, thus, available to be modified by an attacker.

By contrast, in Applicant's system the web content stored on the public server is protected by being encrypted. The backup web content is protected from attack because it is not directly accessible from the public server and, thus, not accessible by an attacker. The backup web content is provided to a private server which is separated from the public server by a firewall. When unauthorized modification of the encrypted content on the public web server is detected, then the encrypted copy can be restored by sending a request to the protected private server. No combination of Gerson with Bianco and Blickenstaff and Menzes teaches such a system wherein the public content is protected by encryption and the private content is protected behind a firewall.

Moreover, none of the cited reference teach or suggest that the authentication header data includes information regarding the file name, file size, file date and file location as recited in Claims 18 and 22 and their dependents.

Regarding Claim 16, the cited prior art does not teach or suggest the anti-alteration system as recited in Claim 15, further comprising a real-time-check module configured to use symmetric-key encryption to decrypt one or more of the safe-web-files when the web visitor's request is received.

Regarding Claim 17, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 16, wherein the symmetric-key encryption is selected from a group consisting essentially of DES, 3DES and AES.

Regarding Claim 18, the cited prior art does not teach or suggest an anti-alteration system for web-content having a public-web-server configured to store safe-web-contents that have been provided with header information including a MAC (Message Authentication Code) generated from the original web-content, and properties of the original-web-content including, name, size, date, and location thereof, a private-web-server configured to store the original web-content the public-web-server provided to the private-web-server through a firewall, the private-web-server configured to separate the header information from a requested safe-web-file, and using the MAC (Message Authentication Code) included in the header information to check an authenticity of the safe-web-file, and the public-web-server configured to add new header information to the original web-content to create a new safe-web-file on the private-web-server computer when an unauthorized alteration of the safe-web-file is detected, wherein the new safe-web-file is sent to the public-web-server computer to automatically restore the altered safe-web-filed.

Regarding Claim 19, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 18, further comprising a real-time-check module used on the public-web-server computer for linking to an authentication module, wherein the authentication module is configured to provide authentication of the safe-web-file in response to a request received from the web visitor though http protocol.

Regarding Claim 20, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 19, wherein the real-time-check module uses a message authentication technology using chaos theory to check whether the safe-web-content has been altered.

Regarding Claim 21, the cited prior art does not teach or suggest he anti-alteration system, as recited in Claim 18, wherein the real-time-check module that is configured to link the public-web-

server services by using at least one message authentication technology selected from a group consisting essentially of MD4, MD5, and SHA.

Regarding Claim 22, the cited prior art does not teach or suggest an anti-alteration system for web-content having a public-web-server computer, configured to store safe-web-files which have been encrypted from original web-contents and have been provided with header information, the header information including a MAC (Message Authentication Code) generated from authentication checking the original web-content and properties including name, size, date, and storage location thereof, a private-web-server computer which retains the original web-content and which is provided to the public-web-server computer through a firewall, a real-time-check module, in response to a web visitor's request safe-web file, the real-time-check module configured to separate the ~~a~~ header information from the safe-web-file using a MAC (Message Authentication Code) included in the header information to authenticate the safe-web-file by comparing the header information with separate header information, and a recovery module, when an unauthorized alteration of the safe-web-file is detected, the recovery module configured to encrypt the original web-content and add header information to the original web-content to create a new safe-web-file on the private-web-server computer, sending the new safe-web-file to the public-web-server computer to automatically restore the safe-web-file which has been altered.

Regarding Claim 23, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 22, wherein the recovery module uses chaos encryption technology to do encryption and decryption.

Regarding Claim 24, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 22, wherein the real-time-check module is configured to provide authentication of the safe-web-file in response to a request received from the web visitor though http protocol.

Regarding Claim 25, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 23, wherein the real-time-check is configured to use a symmetric-key encryption to decrypt the safe-web-contents in response to the web visitor's request.

Regarding Claim 26, the cited prior art does not teach or suggest the anti-alteration system, recited in Claim 25, wherein the symmetric-key encryption is selected from a group consisting essentially of DES, 3DES, RC4 and AES.

Regarding Claim 27, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 24, wherein the real-time-check module uses a message authentication technology using chaos theory to check whether the safe-web-content has been altered.

Regarding Claim 28, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 24, wherein the real-time-check module uses at least one of MD4, MD5, and SHA for message authentication.

Accordingly, Applicant asserts that Claims 16-28 are allowable over the prior art, and Applicant requests allowance of Claim 16-28.

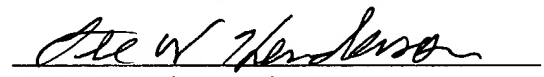
SUMMARY

Applicant respectfully assert that Claims 1-28 are in condition for allowance, and Applicant request allowance of Claims 1-28. If there are any remaining issues that can be resolved by a telephone conference, the Examiner is invited to call the undersigned attorney at (949) 721-6305 or at the number listed below.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: December 22, 2005

By: 

Lee W. Henderson Ph.D.
Registration No. 41,830
Attorney of Record
Customer No. 20,995
(949) 760-0404

2048296_3
122205